AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Apartment REDACTED West Street,
New York, New York

Case No. 16 MAG 0204

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
Apartment 37E, 10 West Street, New York, New York and any closed containers and any items therein

located in the Southern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

PLEASE SEE ATTACHED AFFIDAVIT AND EXHIBITS

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
15 U.S.C. 78j(b) & 78ff, and 18 U.S.C. 1341, 1343, 1346	Securities fraud, mail and wire fraud.

The application is based on these facts:

PLEASE SEE ATTACHED AFFIDAVIT AND RIDER.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Keith Garwood, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: JAN 26 2012

Judge's signature

HON. RONALD L. ELLIS
United States Magistrate Judge
Southern District of New York
Printed name and title

City and state: NY, NY

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

12 MAG 0204

- -X
IN THE MATTER OF THE APPLICATION :
OF THE UNITED STATES OF AMERICA :
FOR THE ISSUANCE OF A SEARCH :
WARRANT FOR THE PREMISES DESCRIBED :
AS APARTMENT REDACTED WEST STREET, :
NEW YORK, NEW YORK 10004, AND ANY :
CLOSED CONTAINERS AND ANY ITEMS :
THEREIN :
:
:
- - - - - - - - - - - - - - - - - - - X

SEALED AFFIDAVIT

STATE OF NEW YORK)
COUNTY OF NEW YORK : ss:
SOUTHERN DISTRICT OF NEW YORK)

KEITH GARWOOD, being duly sworn, deposes and says:

1. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") for approximately 2 years. Before that, I was private banker at J.P. Morgan Chase in New York, New York. I am currently assigned to a squad within the FBI that investigates financial fraud, including securities fraud and related offenses. I have received training regarding the securities industry, accounting methods, and financial fraud. I have participated in numerous financial fraud investigations. I have also participated in the execution of search warrants in non-financial fraud investigations.

2. I am participating in an ongoing investigation of New York Global Group, Inc. ("NYGG-USA"), a Delaware corporation with offices in New York, New York; NYGG-USA's chief executive officer, a naturalized U.S. citizen named Benjamin Wey ("Wey");

Wey's sister, T W , a/k/a "S W ," a/k/a "W T Y ," a Chinese citizen; Benjamin Wey's wife, M W ("Michaela Wey"); various entities owned and/or controlled by Wey and/or T W ; and other entities and individuals. The information contained in this affidavit is based on my own knowledge as well as information obtained from other sources, including, among other things, my conversations with law enforcement officials and my familiarity with the search warrant and sealed affidavit for the search of the Offices of New York Global Group, Inc., excluding the office of James Baxter, Esq., ("the NYGG-USA Office Premises") filed in the Southern District of New York, 12 Mag. 0182, and signed by the Honorable Michael H. Dolinger on or about January 24, 2012. The affidavit in support of that application ("Komar Affidavit") is attached hereto as Exhibit D and is incorporated by reference herein. The search warrant for the NYGG-USA Office Premises signed by Judge Dolinger is attached hereto as Exhibit E.

3. Because this affidavit is being submitted for the limited purpose of establishing probable cause, I have not included details of every aspect of this investigation or every fact that I know about the investigation. Moreover, where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part. To the extent that there are assertions

herein concerning dates and numbers, they are approximations based upon information and evidence gathered to date.

4. This affidavit is respectfully submitted, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, in support of the Government's application for a search warrant for Apartment REDACTED West Street, New York, New York, ("the Wey Apartment"), and any closed or locked cabinets, briefcases, and other containers kept therein, including computers, internal and external hard drives, flash drives, diskettes and other magnetic storage media, and files, data and information contained thereon, used to store names, telephone numbers and addresses and other information, including but not limited to personal digital assistants such as iPhones, iPads, Blackberrys, smartphones, and cellphones (collectively the "PREMISES"). There is probable cause to believe that there is located within the PREMISES, certain books, records, and other documents, which constitute evidence of the commission of, or are designed as a means of the violation of, or are contraband or the fruit of the violation of, the federal securities laws and mail and wire fraud laws, including Title 15, Sections 78j(b) and 78ff, and Title 17, Code of Federal Regulations, Section 240.10b-5 (securities fraud) and Title 18, United States Code, Sections 1341, 1343 and 1346 (mail and wire fraud), as described in detail in the Komar Affidavit (Exhibit D attached hereto).

THE PREMISES

5. The PREMISES consists of Apartment REDACTED West Street, New York, New York. On or about January 25, 2012, I spoke with a law enforcement official who advised me that REDACTED West Street, New York, New York is marked "The Residences at the REDACTED " On the REDACTED Floor of REDAC West Street, the door to apartment REDACTED is clearly marked REDACTED. On or about January 25, 2012, a law enforcement agent went to the PREMISES and served two grand jury subpoenas on Mi We and had a brief discussion with her about the subpoenas. This agent discussed the PREMISES with security officials of REDACTED Street and learned that the PREMISES has two floors.

PROBABLE CAUSE TO BELIEVE THAT THE PREMISES CONTAINS EVIDENCE OF A FRAUD AND MARKET MANIPULATION SCHEME

6. I know from my participation in this investigation that Wey has caused documents that are central to this investigation to be sent to the PREMISES. As described in paragraph 19(d) of the Komar Affidavit, Benjamin Wey caused Interwest Stock Transfer to send one or more sets of Deer Consumer Products, Inc. ("Deer") stock certificates for new round-lot shareholders to be sent to the PREMISES.

7. On or about January 25, 2012, I participated in the search of the NYGG-USA Office Premises pursuant to the warrant signed by Judge Dolinger on or about January 24, 2012. While

inside the NYGG-USA Office Premises, I interviewed two current employees of NYGG-USA ("CS-3" and "CS-4"). CS-3 advised me that M W is the office manager and bookkeeper of NYGG-USA, that she does the bookkeeping from "Ben's home," and that she sometimes mails checks. CS-4 advised me that M W works "from home" and takes care of the payroll; that Benjamin Wey signs checks; and that M W lives at the " ." I know from conversations with another law enforcement agent that two other NYGG-USA employees provided substantially similar information to the FBI on or about January 25, 2012.

8. Another law enforcement agent has advised me that he has obtained records from Paychex, the payroll management firm, showing that M W was, at least as of in or about 2011, a salaried employee of NYGG-USA who is paid approximately $2,000 every two weeks. Paychex records further show that M W is the contact person at NYGG-USA for Paychex. In or about December 2011, an employee of Paychex confirmed that M W is Paychex's contact person for NYGG-USA.

9. As stated in paragraph 9 of the Komar Affidavit (Exhibit D), according to an SEC filing dated July 20, 2005, NYGG-USA was, least at that time, wholly owned by M W , who purportedly served as NYGG-USA's only other executive officer at or about that time.

10. I know from my conversations with law enforcment officials and my review of the Komar Affidavit that Benjamin Wey and M W are married and that they live at the PREMISES.

11. Based on my training and experience, participation in this investigation, my review of the Komar Affidavit, particularly paragraph 35(b), and other sources, I know that, to perform the accounting, payroll, and general office management functions for NYGG-USA, which has multiple employees and complex international business operations, M W would need access to the full range of NYGG-USA's financial and business records, either in hard copy, electronic copy on computers or other storage devices, and/or through remote access to NYGG-USA's offices. For instance, to maintain the books and records of NYGG-USA and manage the office generally, M W would need immediate access to NYGG-USA's books, records, account statements, contracts, correspondence, personnel files, state and federal tax returns, invoices, receipts, and/or other categories of NYGG-USA's business records that are described in paragraphs 35 and 40 of the Komar Affidavit and Exhibit A to this affidavit. Access to full range of such records would be necessary to maintain orderly financial records and manage the wide-ranging affairs of the NYGG-USA office, among other things. In addition, it would be necessary to for M W to have remote access to the full range of NYGG-USA's business records in her capacity

as office manager. I know from my training and experience that business executives such as Benjamin Wey (as well as office managers like M W) frequently access the computer systems of their places of business through remote internet access in order to work from home. As described below in paragraph 17 of this affidavit, remote access to a computer server is likely to leave traces of data on any computer workstation that is used for this purpose. In addition, it is likely that a computer workstation at home is used for e-mail communication to and from NYGG-USA's offices, or to/from other locations in furtherance of NYGG-USA's business operations. Based on the Komar Affidavit, there is probable cause to search any such communications or documents described in this paragraph that may be found on the PREMISES.

12. As described in paragraph 14 of the Komar Affidavit, (Exhibit D), one of Wey's nominees, T W , has transferred large sums of money to Wey's wife, M W , including wire transfers that were divided into increments less than $10,000 to avoid raising suspicion. One or more bank accounts held in the name of M W have addresses listed as P.O. Box 663, New York, New York. I know from my review of the Komar Affidavit and my participation in this investigation that this P.O. Box location is close to the PREMISES. I know from my training and experience that individuals often keep bank records relating to

personal accounts held in their own name at home. Because the P.O. Box location is close to the PREMISES, there is even greater reason to believe that such bank records may be found at the PREMISES.

MATERIALS TO BE SEARCHED AND SEIZED

13. For the reasons set forth above, I submit that there is probable cause to believe that the PREMISES contains fruits, instrumentalities, and evidence related to the above described violations of federal law.

A. Categories of Records

14. Based upon the facts set forth above, as well as my training and experience, I know that individuals involved in securities fraud and market manipulation schemes frequently maintain, for substantial periods of time, the following sorts of materials which evidence the operation of such schemes:

a. Financial records, including banking and brokerage firm account statements, checks, and transaction records, wire transfer instructions and similar documents concerning or reflecting movements of funds, account and account holder information, check numbers, account numbers and Federal Reserve routing numbers;

b. Personal financial records, including banking and brokerage firm account statements, checks, and transaction records, wire transfer instructions and similar documents

concerning or reflecting movements of funds, account and account holder information, check numbers, account numbers and Federal Reserve routing numbers;

c. Telephone bills, telephone message pads, notes, memoranda and other records of internal and external communications;

d. Correspondence, audio tapes, and video tapes;

e. Hotel, airline and credit card receipts reflecting the dates and locations of meetings or travel to meetings;

f. Photographs, address books, Rolodexes, diaries, income tax returns and calendars;

g. Marketing materials, including offering materials, private placement memoranda, sales scripts, investor "lead" lists, investment agreements, financial statements, and other documents concerning, relating to, or describing securities used to entice potential buyers of securities;

h. Documents identifying owners of securities, including transfer agent records, stock certificates, investor lists, investor files, investment subscription agreements, copies of checks received from or sent to investors, copies of account statements sent to investors, copies of correspondence sent to and received from investors, Federal Express, DHL or other records reflecting mailings by private commercial carriers and the U.S. Postal Service, and other documents concerning or

reflecting the identities and participation of investors in such schemes;

i. Documents reflecting the ownership of properties that were purchased with the proceeds of the fraud, including but not limited to houses, apartments, cars, and jewelry, including purchase and sale agreements, deeds, mortgage documents, and other real estate closing documents;

j. Identification documents and other documents which may reflect the identities of persons affiliated with the entities involved in the fraudulent scheme;

k. Corporate documents reflecting the ownership, structure, and relationships among the entities involved in the fraudulent scheme, including incorporation documents, inter-company agreements, lists of partners and stockholders, organizational charts, and corporate resolutions and bylaws; and

l. As described in further detail below, computers, flash drives, internal and external hard drives, compact discs, diskettes and other magnetic storage media, and files, data and information contained thereon, used to store names, telephone numbers and addresses, and other information, including but not limited to personal digital assistants such as iPhones, iPads,

Blackberrys, smartphones, and cellphones, as well as drafts and final versions of documents and correspondence.[1]

15. Based upon my training and experience I also know that individuals involved in securities fraud schemes frequently maintain custody of documents and records of the sort described above, within closed and/or locked cabinets, briefcases and other containers kept within their homes, as well as upon their persons.

B. Names of Relevant Individuals and Entities

16. Based on the facts set forth in this affidavit, there is probable cause to believe that one or more the categories of records described in paragraphs 35 and 40 to the Komar Affidavit will contain information relating to one or more of the following individuals and entities described in this affidavit, such as NYGG-USA, Benjamin Wey, M W , T W , and others listed in Exhibit B to this affidavit, which is incorporated by reference herein. In other words, I am seeking authorization to search the entirety of the PREMISES, for the categories of records described in paragraphs 35 and 40 of the Komar Affidavit and Exhibit A to this affidavit that relate to the individuals and entities described in Exhibit B of this affidavit.

[1] Assuming computers are found at THE PREMISES, the FBI plans to follow the methodology described in Exhibit C to this affidavit in connection with their search.

C. Searches and Seizures of Computer Systems

17. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a desktop computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an

electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Thus, notwithstanding Wey's instructions to his staff that they delete electronic files from their hard drive and store relevant files only on their flash drives, deleted electronic files may still exist on individual desktop computers and/or any computer server that may be in use. In addition, the insertion of a flash drive itself results in a unique log entry on a desktop computer that identifies the specific flash drive that was inserted, and the use of a flash drive to house an e-mail program may leave residue on a hard drive.

18. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including internal and external hard disk drives, flash drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and

software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the

equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 160 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 80 million pages of data, which, if printed out, would result in a stack of paper over four miles high. Further, a 160 GB drive could contain as many as approximately 150 full run movies or 150,000 songs.

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort

through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

19. In light of these concerns, I hereby request the Court's permission to search, copy, image and seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the image or hardware for the evidence described, in the manner described in Exhibit C to this affidavit.

CONCLUSION

20. Based upon the foregoing, I respectfully submit that there is probable cause to believe that there are currently concealed within the PREMISES, the records and articles described in paragraphs 35 and 40 to the Komar Affidavit, this affidavit, and Exhibit A to this affidavit. Moreover, there is probable cause to believe that the items described in paragraphs 35 and 40 of the Komar affidavit, this affidavit, and Exhibit A to this affidavit constitute evidence of securities fraud and wire fraud, in violation of Title 15, Sections 78j(b) and 78ff, and Title 17, Code of Federal Regulations, Section 240.10b-5, and Title 18 United States Code, §§ 1341, 1343 and 1346, among other crimes.

21. Based upon all of the foregoing, I respectfully request that a warrant be issued for the search of the PREMISES as set forth above, as further set forth in Exhibits A, B, and C to this Affidavit.

KEITH GARWOOD
Special Agent
Federal Bureau of Investigation

JAN 26 2012

Sworn to before me this
____th day of January 2012

UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

HON. MICHAEL H. DOLINGER
United States Magistrate Judge
Southern District of New York

12 MAG 0204

SEALING ORDER

David B. Massey affirms as follows:

1. I am an Assistant United States Attorney in the Office of Preet Bharara, United States Attorney for the Southern District of New York, and, as such, I am familiar with this matter and the instant application.

2. In light of the confidential nature of the continuing criminal investigation, the Government respectfully requests that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, in order to avoid premature disclosure of the investigation which could inform potential criminal targets of law enforcement interest, resulting in their flight from justice and/or the destruction of evidence, except that the Government may without further Order of this Court provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and may disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York
January 25, 2011

PREET BHARARA
United States Attorney
Southern District of New York

By: _____
David B. Massey
Assistant United States Attorney
Southern District of New York

JAN 26 2012

SO ORDERED:

_____
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

HON. MICHAEL H. DOLINGER
United States Magistrate Judge
Southern District of New York

EXHIBIT A

PROPERTY TO BE SEIZED AT THE PREMISES KNOWN AND DESCRIBED AS APARTMENT REDACTED WEST STREET, NEW YORK, NEW YORK 10004, and any closed or locked cabinets, briefcases, and other containers kept therein, including computers and electronic storage devices (collectively, "the PREMISES"):

1. Financial records concerning the individuals and entities listed in Exhibit B, which is incorporated by reference herein, including banking and brokerage firm account statements, checks, and transaction records, wire transfer instructions and similar documents concerning or reflecting movements of funds, account and account holder information, check numbers, account numbers and Federal Reserve routing numbers;

2. Personal financial records of any individuals named in Exhibit B or of any employees, agents, or shareholders of any of the entities listed in Exhibit B, including banking and brokerage firm account statements, checks, and transaction records, wire transfer instructions and similar documents concerning or reflecting movements of funds, account and account holder information, check numbers, account numbers and Federal Reserve routing numbers;

3. Telephone bills, telephone message pads, notes, memoranda and other records of internal and external communications between, among, or relating to any of the individuals and entities listed in Exhibit B;

4. Correspondence, audio tapes, and video tapes concerning any of the individuals and entities listed in Exhibit B;

5. Hotel, airline and credit card receipts reflecting the dates and locations of meetings or travel to meetings concerning any of the individuals and entities listed in Exhibit B;

6. Photographs, address books, Rolodexes, diaries, income tax returns and calendars concerning the operations and management of any of the individuals and entities listed in Exhibit B;

7. Computers, flash drives, internal and external hard drives, diskettes and other magnetic storage media, and files, data and information contained thereon, used to store names, telephone numbers and addresses, and other information, including but not limited to personal digital assistants such as iPhones, iPads, Blackberrys, smartphones, and cellphones, as well as

drafts and final versions of documents and correspondence, used by, or used in connection with the individuals and entities listed in Exhibit B. If computers, computer-related equipment, and other electronic devices are found on the PREMISES, the FBI will employ the methodology set forth in Exhibit C, which is incorporated by reference herein, with respect to their search;

8. Marketing materials relating to any of the individuals and entities listed in Exhibit B, including offering materials, private placement memoranda, sales scripts, investor "lead" lists, investment agreements, financial statements, and other documents concerning, relating to, the purchase or sale of securities;

9. Documents identifying shareholders or investors in the entities listed in Exhibit B, including transfer agent records, stock certificates, investor lists, investor files, investment subscription agreements, copies of checks received from or sent to investors, copies of account statements sent to investors, copies of correspondence sent to and received from investors, Federal Express, DHL or other records reflecting mailings by private commercial carriers and the U.S. Postal Service, and other documents concerning or reflecting the identities and participation of investors in such schemes;

10. Documents reflecting the ownership by the individuals and entities listed in Exhibit B of real properties and personal property purchased with the proceeds of fraud, including but not limited to houses, apartments, cars, boats, and jewelry, including purchase and sale agreements, deeds, mortgage documents, and other real estate or other property closing documents;

11. Identification documents and other documents which may reflect the identities of persons listed in Exhibit B or persons affiliated with the entities listed in Exhibit B; and

12. Corporate documents reflecting the ownership or structure of, or relationship between and among, any of the entities listed in Exhibit B, including incorporation documents, inter-company agreements, lists of partners and stockholders, organizational charts, and corporate resolutions and bylaws.

EXHIBIT B

INDIVIDUALS AND ENTITIES

New York Global Group, Inc. ("NYGG-USA"),
a/k/a New York Global Capital

Benjamin Wey, a/k/a Benjamin Wei,
a/k/a Tianbing WEI, a/k/a WEI Tianbing

T W ., a/k/a T Y W , a/k/a S W , a/k/a W T Y

Y W , a/k/a W Y

M W , a/k/a M We , a/k/a M P

M P , a/k/a M P

Bodisen Biotech, Inc.

AgFeed Industries, Inc.

Smartheat, Inc., f/d/b/a Pacific Goldrim Resources

J J W

Deer Consumer Products, Inc., f/d/b/a Tag Events Corporation

Y I.

CleanTech Innovations, Inc., f/d/b/a Everton Capital Corp.

Bei Lu, a/k/a Lu Bei

Nova Lifestyle, Inc.

Capital Properties, Inc.

P.O. Box 663, New York, New York, 10274-0663

Guo Sheng, Ltd.

Strong Growth Capital, Ltd.

York Capital Management, Ltd.

Han Hua, Ltd.

Wolf Enterprises, Ltd.

Advantage Consultants, Ltd.

Finchley International Investments

M L , a/k/a M L , a/k/a L M

New York Global Group (Asia), Ltd.

Tianjin NYGC Investment Consulting Co., Ltd.

Y H , a/k/a H Y

Z C , a/k/a C Z

W J , a/k/a J W

S N H , a/k/a N H

D X , a/k/a X D

Y X Y , a/k/a X Y Y

L Y , a/k/a Y L

Seaboard Securities, Inc.

A D , .

A D , .

First Merger Capital, Inc.

First Merger Capital (Delaware), Inc.

W S

T H

G D

M G

A V

S M. B

G L. C

A C

S C

F: D

M I

J C. I

V F

J B. G

B H

E I

S A. J

A K

B K

W M

M L. M

E M

A N

J R. O

T R

M R

D S

N S

J J. S

L T

Ca V

F V

RRZ Management

R Z

R S

I N

Interwest Stock Transfer

H W , a/k/a "J. W "

K W

B W

G W

L W

N W

K I. W

D W

F W

A W

S W

K W

J W

R N

E N

A S

S S

E (L) S

B S

S S

J A

A: A

N A

P A

K V

T F

R S

T: M

T H

K H

M H

S U

L U

N U

C U

J C:

B C

K C

C C

D J

W J

A D

L A

J A

K R D

S D

F P

N P

J B

N N

E (E) N

J N

K N

G V

A V

J S

C S

P P

M R

M R

T P

J V

C V

A V

W U

M U

F R

A R

F R

J R

B D

G D

M

Y Z

J S

K H

E K

B K

L Y

W

W N

H

Z G

B W

W Y

D W

S H

L J

E M

Q I

W Z

W Y

S P

M K

J G

B M

K P

J G

Z P

A C

G C

P G

A L

P Q

R J

J R

N R

M R

D R

J R

J W

M A W

A M

R B

Es S

H A

R E

Da M

S M

S M

C A

Li Xi

J H

H C

Gı M

J N

Ja S

P S

G S

N S

R S

V C

C C

T C

Fı C

O G

La T

J H

B C

Q M

V E

G E

D E

El G

EXHIBIT C

METHODS TO BE USED TO SEIZE AND SEARCH COMPUTERS AND COMPUTER-RELATED EQUIPMENT

1. In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing this search warrant will employ the following procedure:

a. Upon securing THE PREMISES, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will make an initial review of any computer equipment and storage devices to determine whether these items contain contraband and whether these items can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data.

b. If the computer equipment and storage devices cannot be searched on-site within a reasonable amount of time and without jeopardizing the ability to preserve the data, and if the computer equipment and storage devices do not contain contraband, then the computer personnel will determine whether it is practical to copy the data during the execution of the search in a reasonable amount of time without jeopardizing the ability to preserve the data.

c. If the computer personnel determine that these items contain contraband, or that it is not practical to perform an on-site search or make an on-site copy of the data, then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review. The computer equipment and storage devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

d. The analysis of electronically stored data, whether performed on-site or in a separate, controlled environment, may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); "opening" or reading the first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to

discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "key-word" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

2. Any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offense, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offense specified above.

3. In searching the data, the computer personnel may examine all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.[1]

4. If the computer personnel determine that the computer equipment and storage devices are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(b), the government will return these items, upon request, within a reasonable period of time.

5. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above:

a. Any computer equipment and storage device capable of being used to commit, further or store evidence of the offenses listed above;

b. Any computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;

---

[1] Agents will have procedures in place to segregate any potentially privileged materials or files.

c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, flash drives, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.